Journal of Fuzzy Extension and Applications

www.journal-fea.com

J. Fuzzy. Ext. Appl. Vol. 6, No. 1 (2025) 59–70.

Paper Type: Research Paper

Fuzzy Logic Based Social Trust Computation Scheme in Flying Ad-hoc Network

Joydeep Kundu[1], Sahabul Alam[1], Arindam Dey[2,*]

[1] Department of Computer Science and Engineering, Brainware University, Barasat, Kolkata-700125, West Bengal, India; joydeep.1988kundu@gmail.com; sahabul2009@gmail.com.
[2] School of Computer Science and Engineering, VIT-AP University, Amaravati, Andhra Pradesh-522237, India; arindam84nit@gmail.com.

Citation:

Received: 21 Februray 2024 *Revised: 2 April 2024* *Accepted: 10 June 2024*	Kundu, J., Alam, S., & Dey, A. (2025). Fuzzy logic based social trust computation scheme in Flying Ad-hoc network. *Journal of fuzzy extension and applications*, *6*(1), 59-70.

Abstract

The Flying Ad Hoc Networks (FANETs) are becoming more popular in civic security, military, and multipurpose applications. Owing to its wireless nature and infrastructure-less architecture, the network has some additional security concerns that must be resolved before the system performs worse. Noncooperative drones might introduce harmful and erroneous data, reducing the network's trustworthiness and throughput. Therefore, in the context of trust score, a trustworthy inter-UAV data communication can be achieved by creating a malicious node within the network. This paper describes a social trust computation scheme for clustered-based FANET, which utilises a reputable methodology to separate malicious UAVs within FANET. The mathematical analysis yielded by the proposed scheme is based on fuzzy logic, and it exhibits superior performance in terms of reliability for the existing schemes under adverse conditions. The primary goal of this research is to build social trust scores about the member drones within FANET, which will aid in isolating malicious drones and improve more than 70% accuracy in terms of the packet delivery ratio and average delay concerning other existing approaches.

Keywords: Cluster, FANET, Leader drone, Likelihood.

1 | Introduction

A group of Unmanned Aerial Vehicles (UAVs) or drones that coordinate to carry out designated tasks are part of the Flying Ad Hoc Network (FANET) [1]. These UAVs are connected via wireless communication mediums without any support in creating a fundamental framework [2]. Fuzzy logic, which can handle

Corresponding Author: arindam84nit@gmail.com
https://doi.org/10.22105/jfea.2024.445025.1385

complicated situations and evaluate drone behaviour, is recommended for trust computing. An Internet of Things (LoT) infrastructure that uses a Raspberry Pi processing unit to gather greenhouse data and a low-cost wireless sensor network to monitor and regulate greenhouse irrigation and climate is proposed in [3].

To enable autonomous UAV flying and control within FANET, an advanced automation system that can be programmed dynamically or with pre-programmed flight plans is ideally employed. In terms of application, they are adaptable and flexible. It is suggested that two centralised optimisation algorithms, a greedy approach for adding new relay UAVs to the topology, and an alternating optimisation strategy for routing pathways and relay UAV placements to create a workable FANET topology with the fewest possible relay UAVs in [4]. It leverages graph-convolution for historical characteristics, and inter-UAV communication is described in [5]. It is a stochastic strategy, lowers training costs, and facilitates distributed online learning. It classifies the dangerous environment of UAVs, emphasising security and privacy issues using FANET connections, described in [6].

Therefore, research is needed to secure FANETs using little resources. Prior studies conducted in ad-hoc network domains have demonstrated that employing more dependable algorithms is generally beneficial in providing security to ad hoc networks against various attacks. Drones have a variety of uses in wireless networks since their unique features and capabilities improve network efficiency and open up new application possibilities. In rural or disaster-affected locations where traditional infrastructure is nonexistent or destroyed, drones can serve as airborne base stations or relays to expand wireless coverage. Particularly at busy events or metropolitan areas, drones with communication equipment can unload data traffic from overloaded terrestrial networks, offering more capacity and enhanced connection. Drones with cameras and sensors may be used for surveillance, giving real-time monitoring over big regions for environmental monitoring, traffic control, and security.

As a result, trust management is workable because it increases the dependability of the involved drones. This setting aims to develop a reliable computational method for ad-hoc networks that can be used with FANETs. A UAV can be autonomous, guided by a remote controller, or both. It communicates across the channel without any crew or passengers on board. The ability of a node to join or exit a network independently of other nodes creates an opportunity for eavesdroppers to use malicious mechanisms. The goal of malicious nodes is to reduce the limited network resources, such as nodes' bandwidth, power consumption, and battery life, which shortens the network's lifespan. Malicious node behaviour may arise from frequent topology changes in networks with significant node mobility. When malicious nodes use erroneous routing and discard packets, they destroy network resources.

An interceptor can offer its way since the packet transmission process may choose an alternative path. Malicious nodes may be a part of an eavesdropper's network in wireless ad hoc dynamic networks to disrupt communication. A high packet loss rate and frequent alterations indicate the existence of malicious nodes in a network. Limited resource constraints (battery drain, power outage, and bandwidth use) can weaken a network and leave room for the presence of malevolent nodes that engage in misbehaving behaviour among the other nodes. A malicious node may also be present if a packet does not arrive at its intended destination.

It significantly advances the field of FANETs by presenting a unique quality of experience-based fuzzy social trust computation scheme. This scheme improves social trust computation in dynamic aerial networks by including quality of experience parameters, such as performance and reliability, in the trust evaluation procedure. Furthermore, it addresses a fundamental difficulty in guaranteeing the security and stability of FANETs by proposing a way to detect and isolate non-cooperative drones from the network precisely. These contributions open the door for flying FANETs to operate in a more reliable and resilient manner in a range of applications, from disaster relief to surveillance.

The computation of social trust for the FANET network is the most significant and successful among the abovementioned approaches. Several schemes have shown that trust computation may be used to control a network's efficiency. FANET clustering techniques stabilise traffic patterns and loads while extending the lifespan of FANETs.

1.2 | Contribution

The following are this paper's main contributions:

- *Establishment of quality of experience-based fuzzy social trust computation mechanism for flying FANETs.*
- *To identify and separate non-cooperative drones from a dynamic network.*

The paper contains five sections. Sections 2 and 3 describe the literature review and social fuzzy-based trust computation establishment. The result has been analysed and discussed in Section 4. The last section concludes the paper.

2 | Related Work

Researchers have proposed several trust management techniques to maintain FANET's security in the current situation. To identify and create a malicious node, a TBCS [6] uses several fuzzy categorisation techniques and optimises its verification process for UAV trust. The proposed model [6] can efficiently offload tasks to a remote group of drones, which reduces response time by utilising computational resources from additional drone clusters and increases drone operation by distributing the workload equally. Due to the feedback time based on the bio-inspired technique, the offloading strategy works more effectively. The UAV is the cluster leader based on the highest trust values.

The TBCS calculates the drone's trust levels, further synchronising with their real behaviour. It investigates the benefits and drawbacks of both traditional and innovative UAV routing systems for cyber security. It investigates the UAV-based data collection methods, emphasising their potential advantages in terms of flexibility, reducing the LoT connection load, and improving data delivery in [7].

There are two components to a SEEDRP, routing and security against outside interference. It selects an ideal node solely during forwarding, utilising the cross-layer optimisation technique to alleviate several common FANET difficulties. Consequently, it lowers overload by capping the quantity of route request packets and considering FANET energy safety. The goal is to reduce the number of errors in security levels. The energy of the UAV to satisfy situational requirements and produce dependable outcomes has been used to compute the trustworthiness of inter-UAV interactions.

Energy depletion attacks against based and charging systems are evaluated, and mitigating techniques are presented in [8]. A fuzzy approach for classifying and segregating malevolent nodes in FANETs based on reward and punishment mechanisms is described in [9]. It can circumvent the problem of broadcast storm issues while the interest is spreading. Inter-UAV validation was necessary to authenticate a particular drone's legality without sacrificing the specified security criteria.

UAV misbehaviour, both deliberate and inadvertent, have been recorded. A trust-based method is provided that aims to lower mistake ratios while upholding desirable security levels to distinguish between deliberate and inadvertent UAV misbehaviour in UNION [10], which is to minimise error ratios while maintaining security by presenting a context-aware trust-based method to discriminate between purposeful and inadvertent UAV misbehaviour.

It presents a novel packet distribution technique, assesses context, and builds inter-UAV confidence. It chooses a leader drone based on biological processes in using autonomous drones. Its goal was to select the most dependable and competent drone by considering energy economy and versatility. The remaining energy and the distance at a given time are taken into account by the BOLD algorithm [11], which selects the best drone among several. The drones build themselves into numerous clusters according to the mission criteria using the same amount of residual energy, and then they choose a leader drone. The fitness criterion is based on the pair or the separation between the drones and the remaining energy. To advance feedback computation locally or remotely, drone clusters are advised to apply computational offloading.

Adaptive trust techniques were made in [12] to enable secure communication between many drones. Service quality and experience metrics are enhanced using chaotic algae and dragonfly algorithms for cluster selection, management, and inter-cluster data transmission in [13]. It combines unicasting and geocaching routing to forecast intermediate node positions, increase transmission range, track changing topology, and reduce interruption time by utilising 3-D estimates in [14]. A secure, portable key management and authentication-based solution for cloud-assisted UAVs to provide access control and data integrity by blockchain technology is described in [15]. It is divided into two phases, routing and security [16]. The latter phase employs a unique, dynamic key generation system for data security, while the former implements a dynamic routing algorithm for economic data transfer. It evaluates forwarding behaviours and trust values and separates malicious nodes from benign ones using delay about pre-planned route information, classification, and clustering [17]. The car can choose a random pseudonym from a list, maintain anonymity by regularly altering it, and does not require certificates or certificate revocation lists for authentication, as described in [18]. A deep learning-based system is used to diagnose medical purposes like Parkinson's illness described in [19].

Existing schemes find it challenging to control broadcast storm complexity, design optimal drone leader selection methods, guarantee route dependability, include energy efficiency, and suggest technologies to detect and prevent unauthorised drones from entering private areas. These difficulties impede the creation of an effective drone management system. The proposed scheme has addressed the shortcomings of the earlier plans by completing the research gaps. Thus, reducing energy depletion improves Quality of Service (QoS) and provides the best possible plan for using UAVs in a FANET. It is used to secure the UAVs throughout their routes and protect them during data transfer in FANET.

Using a hybrid trust score, the TBCS [9] scheme dynamically selects leader drones to improve UAV network security and efficiency. Fuzzy-based classification increases the detection and isolation accuracy of non-cooperative nodes. Using energy levels and buffer space, the UNION [10] system locates and separates purposeful and inadvertent UAVs. SecRIP [13] uses Dragonfly algorithms to protect UAVs while transmitting data. The proposed scheme identifies deliberate and inadvertent misbehaviour based on energy levels, honesty ratings, and drone movement patterns. It controls data flow, enhances network efficiency, and uses less energy. Misbehaviour is categorised using fuzzy rules, which improves network detection and resolution.

3 | The Proposed Social Trust Calculation Using Fuzzy Logic

The main goal of this technique is to improve social trust computation for cluster-based (intra-cluster, inter-cluster) systems. Another goal is to prevent the selection of malevolent UAVs as both members and leaders. The leader of a clustering environment keeps a matrix-based recommendation trust about its member drones. The process of determining how reliable or trustworthy a system's entities, such as users, agents, or network drones, are is known as trust computation. The computational scheme may efficiently solve the unpredictable and complex nature of trust computation from the social environment by using fuzzy sets, trust calculations, and fuzzy rules.

Regarding computations, linguistic variables show qualitative values like consistency, reliability, etc. It provides three classifications for trustworthiness, i.e., best, neutral, and poor, facilitating a more in-depth evaluation and comprehensible analysis and decision-making procedures. The suggested mechanism divides UAVs into genuine, non-cooperative, and neutral drones. The cluster's leader UAV keeps track of data from its other UAV members. As a result, when a new UAV wants to enter, it transmits a joining message to the leader UAV inside the cluster. So that the person in charge of the request can react to the acknowledgement. In the same way, the base station chooses the legitimate gateways that connect each leader UAV in the network during inter-cluster communication.

Additionally, the server drone (i.e., base station) keeps track of all of its gateways' comments, and each gateway keeps track of the information regarding its lead UAVs. Regarding computations, linguistic variables show qualitative values like consistency, reliability, etc. It provides three classifications for trustworthiness, i.e., best, neutral, and poor, facilitating more in-depth evaluation and more comprehensible analysis and decision-

making procedures. As a result, the base station can quickly determine the social trust score and identify UAV leaders who are dishonest or hostile. The social trust calculation is now explained in *Fig. 1*.

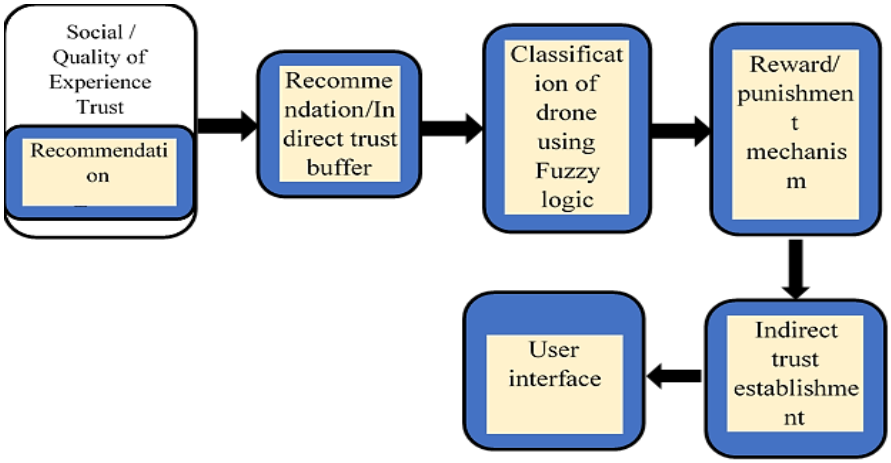

Fig. 1. Proposed methodology for social trust computation.

3.1 | Establishment of a Fuzzy-Based Social Trust Computation Scheme

Leader drones are thought to have a larger memory capacity and require more energy consumption than member drones. Within a clustering environment, the leader drone determines the recommended trust for each member. The direct observation score of each node to a single-member drone makes up the recommendation information, and the direct trust of each drone in the leader determines the weight of the suggestions in our scheme. Moreover, if the drone's direct trust in the leader is below a threshold value (say 0.45), the leader drone discards its recommended value to conserve bandwidth. Assume a cluster consists of n numbers of leaders, including the leader.

The leader thus periodically transmits the request message to $((\text{drone\_n} - 1))$ members. As a result, each member will communicate their trust values to the leader via other members, and the leader will then maintain these values as a matrix ($\text{TR}^{\text{leader}}$) inside a cluster, as illustrated below.

$$\text{TR}^{\text{leader}} = \begin{pmatrix} \text{TR}_{\text{drone\_1,leader}} & \text{TR}_{\text{drone\_1,drone\_1}} & \cdots & \text{TR}_{\text{drone\_1,drone\_n-1}} \\ \text{TR}_{\text{drone\_2,leader}} & \text{TR}_{\text{drone\_2,drone\_1}} & \cdots & \text{TR}_{\text{drone\_2,drone\_n-1}} \\ \vdots & \vdots & \vdots & \vdots \\ \text{TR}_{\text{drone\_n-1,leader}} & \text{TR}_{\text{drone\_1,rone\_n-1}} & \cdots & \text{T}_{\text{rone\_n-1,rone\_n-1}} \end{pmatrix}. \quad (1)$$

The trust scores for each of the leader drone's one-hop neighbours are displayed in the first column of the matrix. As a result, the cluster head's (n-1)th member node's trust score is represented as $\text{TR}_{\text{drone\_n-1,leader}}$. The direct trust values of member nodes towards their neighbour nodes, denoted as $\text{TR}_{\text{drone\_1,drone\_1}}$, $\text{TR}_{\text{drone\_2,leader}}$, respectively. $\text{TR}_{\text{drone\_1,drone\_1}}$, $\text{TR}_{\text{drone\_2,drone\_2}}$ are calculated and indicate the drones' direct trust values towards themselves. As a result, the direct trust value of the member node, say, ith drone towards a jth drone, is generally represented by $\text{TR}_{\text{drone\_i,drone\_j}} \in [1, \text{drone}_n - 1]$. The Bayesian technique described below determines the trust score in leader-to-member recommendations.

The components are the likelihood function, the posterior (updated) distribution, and the prior (previous) distribution based on the Bayesian method. The likelihood function (good and bad feedback) represents the information about the parameters. The posterior (updated) function is created by merging the likelihood function and the prior distribution. In contrast, the preceding distribution provides information that considers the components before viewing the nature of trust.

The function of posterior components (distribution) shows the whole amount seen [18] serves as our inspiration. Assuming a distribution function of Bernoulli with a positive (success) chance of, say, q, is to be monitored separately by $\text{x}_{\text{i}}^{\text{th}}(\text{x}_{\text{drone}_1}, \text{x}_{\text{drone}_2}, \ldots\ldots, \text{x}_{\text{drone}_{n-1}})$ trust values. It can be written as follows:

$$p\left(x_i^{th}|t\right) = r^{x_i^{th}}(1-t)^{\left(1-x_i^{th}\right)}, i \in (1, drone_n - 1), \quad (2)$$

where $TR_{drone\_i,drone\_j}$ is calculated between two neighbour cluster members within such environment and x_i^{th} is the positive (social trust score is more than and equal to the threshold value) or negative (social trust score is less than the threshold value) feedback trust of the ith cluster member. It is assumed that the cluster consists of (n-1) members. The random number r represents the likelihood that a specific occurrence will be successful. The Bayesian reputation system calculates the reputation value using the beta probability(modified) density function [19–23]. Two types of reputation ratings,i.e., good reputation and bad reputation feedback, have been explained by m and n, respectively. The distribution function (continuous) is known as the beta distribution. Thus, the beta distribution's probability expectation value is expressed as

$$Expectation\left(\rho(p|m,n)\right) = \frac{m}{m+n}, 0 \le p \le 1 \,\&\, m,n > 0. \quad (3)$$

For the Bernoulli method, the function of prior components (distribution) with positive feedback, say, p, equals a beta distribution with two provided parameters (good and bad feedback scores). Thus, the beta probability distribution function $p(r|m,n)$ has been represented as follows, using the gamma function (Γ) as a foundation.

$$p(r) = p(r|m,n) = \left[\left(\frac{\Gamma(m+n)}{\Gamma(m)\Gamma(n)}\right)t^{(m-1)}(1-t)^{(n-1)}\right]. \quad (4)$$

The factorial function and the gamma function are strongly related in that $\Gamma(n) = (n-1)!$. A and b represent the total feedback score for the event r. *Eq. (5)* expresses the joint probability function, the revised distribution's like-hood function. Assumed to be separately gathered are the reputation feedback ratings $x_{drone_1}, x_{drone_2}, \ldots\ldots, x_{drone_{n-1}}$. Consequently, the like-hood function is shown as

$$Likehood(t|x_i) = \prod_{i=1}^{n-1} r^{x_i}(1-t)^{(n-1)-x_i}. \quad (5)$$

The like-hood function in the Bayesian approach contains all of the data regarding p, which is derived by direct obervastion from the trust score ratings. Consequently, the like-hood function is shown as,

$$L(t|x_i) = \prod_{i=1}^{n-1} r^{x_i}(1-t)^{(n-1)-x_i}. \quad (6)$$

We now use the Bayes theorem to get the revised posterior distribution. As a result, $p(r|x_i)$ is shown as follows:

$$p(t|x_i) = \frac{p(r)L(t|x_i)}{p(x)} \infty p(t)Likehood(t|x_i), \quad (7)$$

where "∞" denotes "proportional to," meaning that after multiplying the term farthest to the right by a normalising constant value independent of r, the expressions are equivalent.

Therefore, removing the Like-hood functions and multiplicative constants from the previous beta distribution independent of the event r is a helpful method for calculating the posterior distribution. After that, the normalising constant is calculated and displayed below.

$$L(t|x_i) \infty p(t|x_i) \infty p(t)L(t|x_i), \quad (8)$$

where

$$p(t)L(t|x_i) = \left(\left(\frac{\Gamma(m+n)}{\Gamma(m)\Gamma(n)}\right)(t^{m-1})(1-t)^{(n-1)} \right) x_i th(1-t)^{((n-1)-x_i)} = \left(\frac{\Gamma(m+n)}{\Gamma(m)\Gamma(n)}\right) t^{x_i+m-1}(1-t)^{k-x_i+n-2}. \quad (9)$$

Thus the $P(p|t)$ is represented by,

$$P(t|x) = \frac{\Gamma(m'+n')}{\Gamma(m')\Gamma(n')} t^{m'(1-t)^{n'}}, \quad (10)$$

where $m' = x_i + m - 1$ and $n' = k - x_i + n - 2$.

Since the normalising constant in the previous distribution is independent of the event r, it is deleted. It has been seen that the last statement is sufficient for the Beta function (distribution) with m, n. The probability variable p is restricted because when either a is less than 1 or b is smaller than 1, it can never be zero ($P \neq 0$). The prior reputation score is added to the new rating to calculate the adjusted beta probability distribution function. This can be stated as:

$$\text{Expectation}\big(\rho(p|m'', n'')\big) = \left(\frac{m''}{m''+n''}\right) = \left(\frac{m''+1}{m''+n''+2}\right), \quad 0 \leq p \leq 1. \quad (11)$$

We, therefore, compute the leader to members' feedback trust $T^{Recommendation}_{leader,drone\_j}$ applying the beta probability density (modified) function's probability expectation value as follows:

$$T^{Recommendation}_{leader,drone\_j} = \left[\text{xpectation}\big(\rho(p|m'', n'')\big)\right] = \left(\frac{x_i + m}{m+n+k-1}\right). \quad (12)$$

In the preceding equation, the letters m and n represent the cluster members' good and bad reputation scores, respectively. Drone $x_i th$ is the sum of reliable members among the n number of members participating in a cluster. The leader can quickly determine the feedback trust for drone j by applying the abovementioned approach since it keeps track of the trust score for each of its member nodes inside the matrix TR^{leader}. As a result, the leader-to-member recommendation feedback system is straightforward and adaptable.

4 | Simulation and Analysis of the Proposed Scheme

The modelling environment creates drones' positive and negative impacts on the FANET networks [24–27]. OMNeT++'s mobility systems and its traffic patterns allow for the simulation of real-world issues by altering influxes. Drones may be controlled simultaneously because of their scalable infrastructure. The drones are then divided into three categories for experiments, i.e., good, neutral, and bad. Neutral drones seldom commit detrimental or self-serving behaviours, frequently operate optimally, and have fewer resource limitations. The non-cooperative drones are made to operate autonomously and maliciously in FANET. The movement patterns of more than 650 UAVs are randomly generated by waypoints inside a simulated three-dimensional region.

Communication protocols employ constant bit-rate traffic, which may travel at rates of up to 70 km/h. Initial trust value influences cooperative conduct. The movement patterns of more than 650 UAVs are randomly generated by waypoints inside a simulated three-dimensional region. Communication protocols employ constant bit-rate traffic, which may travel at rates of up to 70 km/h. Initial trust value influences cooperative conduct. The value of the simulation parameters is in *Table 1*.

Table 1. Parameters value.

Parameters	Quantity
Area	(1750×1350×800) meter cube
UAVs	650
Length of the packet	4750 bits
Drone's or UAV's positions	Randomly placed
Scheme's mobility	Random waypoint
Traffic managemet technique	Constant Bit Rate
UAV's velocity	20–64 MPS
Window time	35s
Primary trust score	0.475

4.1 | Result Analysis and Discussion

This section investigates the result of the proposed scheme's resilience to assaults on the fuzzy-based social trust computation scheme. It provides security and performance analysis, enforces airspace regulations for UAV operations, assesses verification using many methods, and uses blockchain and smart contract technology, among others [28]. It provides this investigation of UAV kinds, classifications, charging techniques, laws, application situations, difficulties, security concerns, etc [29]. This scheme allows UAV swarms to establish physical security and trust by utilising an optimised route [30]. It presents a new clustering technique based on reward index, speed, and distance to select the leaders and members for best performance [31]. It provides a cooperative underwater target-hunting network, emphasising energy-oriented optimisation of UAV locations, trajectories, and interconnectivity [32].

A safe resource allocation scheme [33] maximises secure energy consumption by separating non-convex issues into convex subproblems and optimising the user association matrix and network parameter allocation. It provides a communication scenario that elects a secure leader based on calculated trust scores for communication and employs a reputable technique to separate harmful UAVs [34]. This is because the system can identify malicious drones and prevent them from achieving their goals. It is assumed that well-performing nodes interact well and provide accurate input. Malicious drones, on the other hand, attempt to conduct badmouthing or garnished assaults.

A more precise definition has been proposed that describes the actions of malicious drones, and mathematical analysis shows how such drones can attempt to obtain an unfair advantage in the social trust computation scheme in the following section. Next, we demonstrate the resilience of our trust system against these types of malevolent attacks. Randomly placed UAVs were scattered around the simulated area. The network has three types of UAVs: excellent, neutral, and bad. A UAV that operates at peak efficiency and adheres to protocols is ideal. The hostile UAVs will attempt to perform detrimental tasks like packet loss, traffic congestion, denial of service, etc.

4.1.1 | Ratio of packet delivery

A drone network is simulated based on network performance evaluation, and the average, lowest, and maximum values of the Packet Delivery Ratio (PDR) are recorded as described in *Fig. 2*. A drone with a PDR greater than expectation (means 90 and above) is regarded as dependable and trustworthy. A drone with a medium PDR (76 and above but less than 90) is deemed unreliable and has a negative reputation. In FANETs, node-level communication consumes significantly more battery power than combined computation and operation. In addition to communication, UAVs need a large battery capacity for flying and independence in the atmosphere.

For this reason, the leader was selected based on the fuzzy-based social trust score. Several criteria are developed to characterise the behaviour of a drone categorisation based on the type of reward. The proposed scheme in *Fig. 2* has a greater PDR than BOLD [11] and UNION [10]. Using the UNION approach, the delivery ratio is 17% at 120 drones and increases to 21% at 140 drones. The suggested plan demonstrates

significant gains from 27% to 41%, while BOLD's boost is more pronounced, going from 22% to 33%. It shows that the suggested scheme is a workable approach for efficient data transfer inside the network.

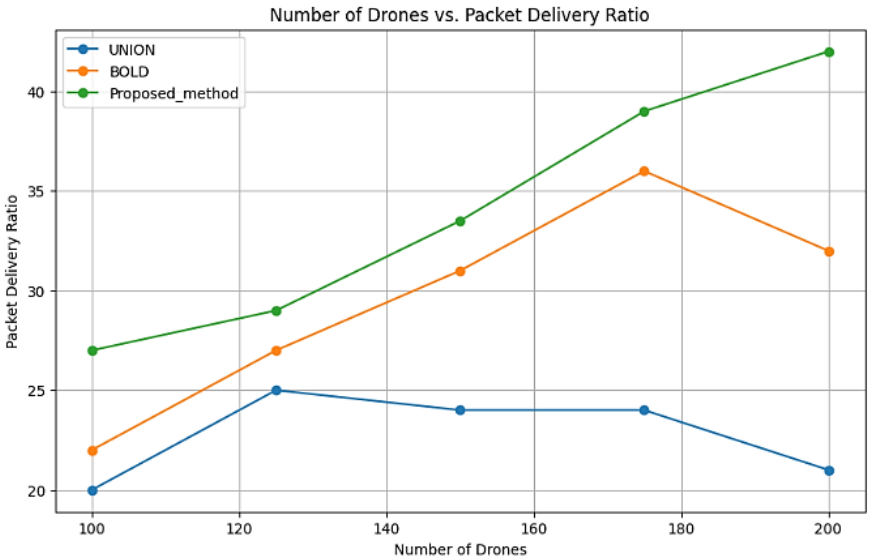

Fig 2. Comparison of packet delivery performance between proposed scheme and existing models.

4.1.2 | Effect of delay

FANET performance is calculated from the delay that occurs during the time of packet transmission to its destination. The primary cause of the delay might be lost packets or heavy traffic. The impact of a delay based on the current methods is explained in *Fig. 3*. No matter how effective the network is, delays will always happen since it is difficult to forecast the network at any given time. The real challenge for the networks is to minimise this latency as much as possible. It will help to maintain the network's service quality. It can retain the lowest possible delay when compared to the other techniques. The BOLD protocol [11] performs exceptionally well compared to the UNION protocol [10]. It can reduce the amount of network delay as compared to the UNION protocol. It tackles the problem of network latency by grouping its networks. The network can be partitioned into clusters using clustering, each under the direction of a leader. The total transmission of each cluster is now under the leader's control.

This system selects the cluster leader using the trust-based clustering technique. There is little delay because the packets are sent as quickly as possible. *Fig. 3* illustrates how energy consumption in the UNION [10] scheme rises steadily with network complexity, from 1.25 seconds to 3.34 seconds and then somewhat declines to 3.12 seconds at 200 drones. In contrast, BOLD [11] indicates that the energy consumption of drones is trending upward, reaching 4.2 seconds at 200 drones from 1.6 seconds at the beginning. On the other hand, the suggested plan demonstrates more efficient energy use, as seen by consistently declining consumption figures for the growing number of drones.

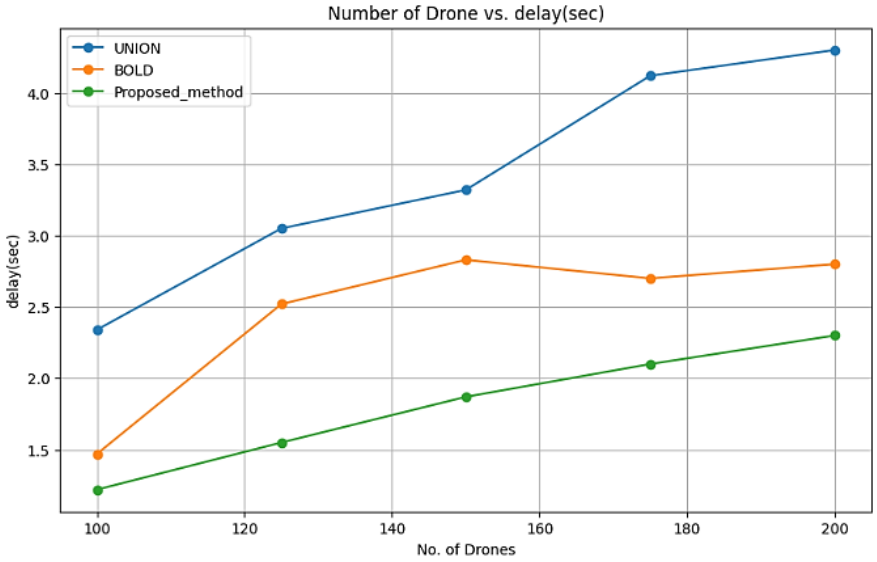

Fig 3. Comparison of delay performance between proposed scheme and existing models.

5 | Conclusion

A new fuzzy-based social trustworthy scheme has been proposed to detect and separate malicious and non-cooperative drones in FANETs. The outcomes confirm that it can distinguish between malicious and non-cooperative nodes. Additionally, as the network size grows, detection accuracy rises, suggesting that the suggested approach is scalable. Moreover, it has been noted that a strong dependence on recommendations, or social trust, results in erroneous trust values. The suggested paradigm reduces links with malicious drones, saving node energy. The proposed trust model has also been compared with existing protocols. The proposed model performs better in the highly dynamic FANET environment than the existing models.

The proposed social trust computation scheme scores better results because it detects and isolates the drones with the help of the recommendation trust score. This score establishes the genuine impact of the nature of drones, but the existing schemes depend on the direct interaction with the neighbour drones within FANET. Drones use radio frequencies for communication (wireless); however, the range of the messages they send can be shortened by obstructions or interference. It might lead to signal degradation, data missing, and poor network connectivity. Drones may operate in networks with low capacity, affecting network connection.

This scheme can be expanded for further research to lower energy usage and improve drone behaviour prediction in FANETs. A machine learning-based dynamic trust computation scheme can investigate the scheme's efficiency using the parameters, i.e., a more significant number of malicious drones and transmission range.

Author Contribution

All the authors are equally contributed to the paper.

Data Availability

The data used in this study are available upon request from the corresponding author.

Funding

The study received no funding.

Conflicts of Interest

All the authors have no conflict of interest.

References

[1] Hosseinzadeh, M., Mohammed, A. H., Alenizi, F. A., Malik, M. H., Yousefpoor, E., Yousefpoor, M. S., … & Tightiz, L. (2023). A novel fuzzy trust-based secure routing scheme in flying ad hoc networks. *Vehicular communications*, *44*, 100665. DOI:10.1016/j.vehcom.2023.100665

[2] Benfriha, S., Labraoui, N., Bensaid, R., Bany Salameh, H., & Saidi, H. (2024). FUBA: a fuzzy-based unmanned aerial vehicle behaviour analytics for trust management in flying ad-hoc networks. *IET networks*, *13*(3), 208–220. DOI:10.1049/ntw2.12108

[3] Benyezza, H., Bouhedda, M., Kara, R., & Rebouh, S. (2023). Smart platform based on IoT and WSN for monitoring and control of a greenhouse in the context of precision agriculture. *Internet of things (netherlands)*, *23*, 100830. DOI:10.1016/j.iot.2023.100830

[4] Liu, Y., Xie, J., Xing, C., & Xie, S. (2023). Topology construction and topology adjustment in flying Ad hoc networks for relay transmission. *Computer networks*, *228*, 109753. DOI:10.1016/j.comnet.2023.109753

[5] Ye, Z., Wang, K., Chen, Y., Jiang, X., & Song, G. (2023). Multi-UAV navigation for partially observable communication coverage by graph reinforcement learning. *IEEE transactions on mobile computing*, *22*(7), 4056–4069. DOI:10.1109/TMC.2022.3146881

[6] Tsao, K. Y., Girdler, T., & Vassilakis, V. G. (2022). A survey of cyber security threats and solutions for UAV communications and flying ad-hoc networks. *Ad hoc networks*, *133*, 102894. DOI:10.1016/j.adhoc.2022.102894

[7] Messaoudi, K., Oubbati, O. S., Rachedi, A., Lakas, A., Bendouma, T., & Chaib, N. (2023). A survey of UAV-based data collection: challenges, solutions and future perspectives. *Journal of network and computer applications*, *216*, 103670. DOI:10.1016/j.jnca.2023.103670

[8] Tlili, F., Fourati, L. C., Ayed, S., & Ouni, B. (2022). Investigation on vulnerabilities, threats and attacks prohibiting UAVs charging and depleting UAVs batteries: assessments & countermeasures. *Ad hoc networks*, *129*, 102805. DOI:10.1016/j.adhoc.2022.102805

[9] Singh, K., & Verma, A. K. (2020). TBCS: a trust based clustering scheme for secure communication in flying ad-hoc networks. *Wireless personal communications*, *114*(4), 3173–3196. DOI:10.1007/s11277-020-07523-8

[10] Barka, E., Kerrache, C. A., Lagraa, N., Lakas, A., Calafate, C. T., & Cano, J. C. (2018). UNION: a trust model distinguishing intentional and unintentional misbehavior in inter-UAV communication. *Journal of advanced transportation*, *2018*(1), 7475357. DOI:10.1155/2018/7475357

[11] Ganesan, R., Raajini, X. M., Nayyar, A., Sanjeevikumar, P., Hossain, E., & Ertas, A. H. (2020). Bold: bio-inspired optimized leader election for multiple drones. *Sensors*, *20*(11), 3134. DOI:10.3390/s20113134

[12] Du, X., Li, Y., Zhou, S., & Zhou, Y. (2022). ATS-LIA: a lightweight mutual authentication based on adaptive trust strategy in flying ad-hoc networks. *Peer-to-peer networking and applications*, *15*(4), 1979–1993. DOI:10.1007/s12083-022-01330-7

[13] Bhardwaj, V., Kaur, N., Vashisht, S., & Jain, S. (2021). SecRIP: secure and reliable intercluster routing protocol for efficient data transmission in flying ad hoc networks. *Transactions on emerging telecommunications technologies*, *32*(6), e4068. DOI:10.1002/ett.4068

[14] Gankhuyag, G., Shrestha, A. P., & Yoo, S. J. (2017). Robust and reliable predictive routing strategy for flying ad-hoc networks. *IEEE access*, *5*, 643–654. DOI:10.1109/ACCESS.2017.2647817

[15] Yu, S., Lee, J., Sutrala, A. K., Das, A. K., & Park, Y. (2023). LAKA-UAV: lightweight authentication and key agreement scheme for cloud-assisted Unmanned Aerial Vehicle using blockchain in flying ad-hoc networks. *Computer networks*, *224*, 109612. DOI:10.1016/j.comnet.2023.109612

[16] Bhardwaj, V., & Kaur, N. (2021). SEEDRP: a secure energy efficient dynamic routing protocol in fanets. *Wireless personal communications*, *120*(2), 1251–1277. DOI:10.1007/s11277-021-08513-0

[17] Zhai, W., Liu, L., Ding, Y., Sun, S., & Gu, Y. (2023). ETD: an efficient time delay attack detection framework for UAV networks. *IEEE transactions on information forensics and security*, *18*, 2913–2928. DOI:10.1109/TIFS.2023.3272862

[18] Moni, S. S., & Manivannan, D. (2022). CREASE: certificateless and reused-pseudonym based authentication scheme for enabling security and privacy in VANETs. *Internet of things (Netherlands)*, *20*, 100605. DOI:10.1016/j.iot.2022.100605

[19] Hammoud, M., Kovalenko, E., Somov, A., Bril, E., & Baldycheva, A. (2023). Deep learning framework for neurological diseases diagnosis through near-infrared eye video and time series imaging algorithms. *Internet of things (Netherlands)*, *24*, 100914. DOI:10.1016/j.iot.2023.100914

[20] Lu, Y., Wen, W., Igorevich, K. K., Ren, P., Zhang, H., Duan, Y., … & Zhang, P. (2023). UAV ad hoc network routing algorithms in space–air–ground integrated networks: challenges and directions. *Drones*, *7*(7), 448. DOI:10.3390/drones7070448

[21] Sharma, B., Obaidat, M. S., Sharma, V., & Hsiao, K. F. (2020). Routing and collision avoidance techniques for unmanned aerial vehicles: analysis, optimal solutions, and future directions. *International journal of communication systems*, *33*(18), e4628. DOI:10.1002/dac.4628

[22] Khan, M. F., Yau, K. L. A., Noor, R. M., & Imran, M. A. (2020). Routing schemes in FANETs: a survey. *Sensors*, *20*(1), 38. DOI:10.3390/s20010038

[23] Xu, M., Xie, J., Xia, Y., Liu, W., Luo, R., Hu, S., & Huang, D. (2020). Improving traditional routing protocols for flying ad hoc networks: a survey. *2020 IEEE 6th international conference on computer and communications, ICCC 2020* (pp. 162–166). IEEE. DOI: 10.1109/ICCC51575.2020.9345206

[24] Mukherjee, A., Dey, N., Kausar, N., Ashour, A. S., Taiar, R., & Hassanien, A. E. (2019). A disaster management specific mobility model for flying ad-hoc network. In *Emergency and disaster management: concepts, methodologies, tools, and applications* (pp. 279–311). IGI Global. DOI: 10.4018/978-1-5225-6195-8.ch013

[25] Kaur, M., Verma, S., & Kavita. (2020). Flying ad-hoc network (FANET): challenges and routing protocols. *Journal of computational and theoretical nanoscience*, *17*(6), 2575–2581. DOI:10.1166/jctn.2020.8932

[26] Pan, H., Liu, Y., Sun, G., Fan, J., Liang, S., & Yuen, C. (2023). Joint power and 3d trajectory optimization for UAV-enabled wireless powered communication networks with obstacles. *IEEE transactions on communications*, *71*(4), 2364–2380. DOI:10.1109/TCOMM.2023.3240697

[27] Beegum, T. R., Idris, M. Y. I., Ayub, M. N. Bin, & Shehadeh, H. A. (2023). Optimized routing of UAVs using bio-inspired algorithm in FANET: a systematic review. *IEEE access*, *11*, 15588–15622. DOI:10.1109/ACCESS.2023.3244067

[28] Alkadi, R., & Shoufan, A. (2023). Unmanned aerial vehicles traffic management solution using crowd-sensing and blockchain. *IEEE transactions on network and service management*, *20*(1), 201–215. DOI:10.1109/TNSM.2022.3201817

[29] Mohsan, S. A. H., Othman, N. Q. H., Li, Y., Alsharif, M. H., & Khan, M. A. (2023). Unmanned aerial vehicles (UAVs): practical aspects, applications, open challenges, security issues, and future trends. *Intelligent service robotics*, *16*(1), 109–137. DOI:10.1007/s11370-022-00452-4

[30] Bansal, G., Naren, Chamola, V., & Sikdar, B. (2022). SHOTS: scalable secure authentication-attestation protocol using optimal trajectory in UAV swarms. *IEEE transactions on vehicular technology*, *71*(6), 5827–5836. DOI:10.1109/TVT.2022.3162226

[31] Khayat, G., Mavromoustakis, C. X., Pitsillides, A., Batalla, J. M., Markakis, E. K., & Mastorakis, G. (2023). On the weighted cluster S-UAV scheme using latency-oriented trust. *IEEE access*, *11*, 56310–56323. DOI:10.1109/ACCESS.2023.3282441

[32] Wei, W., Wang, J., Fang, Z., Chen, J., Ren, Y., & Dong, Y. (2023). 3U: joint design of UAV-USV-UUV networks for cooperative target hunting. *IEEE transactions on vehicular technology*, *72*(3), 4085–4090. DOI:10.1109/TVT.2022.3220856

[33] Bastami, H., Moradikia, M., Abdelhadi, A., Behroozi, H., Clerckx, B., & Hanzo, L. (2022). Maximizing the secrecy energy efficiency of the cooperative rate-splitting aided downlink in multi-carrier UAV networks. *IEEE transactions on vehicular technology*, *71*(11), 11803–11819. DOI:10.1109/TVT.2022.3192298

[34] Kundu, J., Alam, S., & Koner, C. (2022). TCSFANET: trusted communication scheme for fanet system. *2022 international conference on machine learning, computer systems and security (MLCSS)* (pp. 353–357). IEEE. DOI: 10.1109/MLCSS57186.2022.00070